31 PRTS

09/647170

526 Rec'd PCT/PTO 27 SEP 2000

GR 98 P 3222

Ins. A7

~~Description~~

A

Data transfer method

The present invention relates to a method for transferring data between a secure computer, e.g. an error-protected stored-program control, and a number of input/output units via a bus control unit connected to the secure computer and a serial bus system. ~~in which~~ The bus control unit cyclically activates the input/output units connected to the bus system and transfers a multi-bit message to the respective activated input/output unit.

A

A

A data transmission method of this type is known, e.g. by the name AS-i (= activator-sensor interface).

Ins. A2

In industrial automation engineering installations and machinery, hazardous conditions must be reliably identified and the controlled installation or machinery must be rendered secure in such an event. According to the state of the art, dedicated recording, cabling and evaluation systems are mostly used for the transmission of security-related signals of this type.

The use of dedicated recording, wiring and evaluation systems entails in particular high cabling cost, with the inherent risk of incorrect wiring. Efforts are therefore also made to transmit security-related signals via a bus system of this type. However, the security and reliability of the data transfer must not be adversely affected by a bus system of this type.

The security-related signals can be transmitted via a separate, error-protected bus system. However, this

runs counter to the general tendency to minimize the wiring outlay.

DE 43 12 305 A1 discloses a method for transferring data between an error-protected stored-program control and a number of input/output units via a bus control unit connected to the stored-program control and a serial bus system. ~~in which~~ The bus control unit transfers messages to the input/output units connected to the bus system. In this data transfer method, at least one of the input/output units is designed as a security unit. Messages transferred to the security unit are transferred redundantly and are checked to ascertain whether or not they are identical. The transferred messages are interpreted as correct only if they are identical.

A

Ins-A3

The object of the present invention is to provide a further data transmission method by means of which security-related signals can be transmitted via a non-error-protected bus system.

The object is achieved in a data transmission method of the aforementioned type in that at least one of the input/output units is designed as a security unit. The multi-bit message transferred to the security unit has a checkbit. ~~and~~ The security unit interprets the transferred multi-bit message as correct only if the checkbit alternates within a predefined monitoring period.

A

A

An insecure condition is thus avoided - even in the case of non-redundant data transfer - not only if no

further multi-bit messages are transferred, e.g. in the event of failure of the bus control unit, but also if errored multi-bit messages are transferred.

A
A
A

If the security unit is designed as an output unit for activating an output, it may, for example, have a timer. ~~which,~~ A~~a~~t the end of the monitoring period, the timer switches the output to a secure condition. ~~in which~~ T~~t~~he timer is reset with each transfer of a correct multi-bit message.

A
A
A

The data transmission method is even more secure if the security unit can be activated under two different addresses. A ~~a~~ multi-bit message is, in each case, transferred to the security unit under both addresses and the security unit interprets the transferred multi-~~bit message as correct only if the two multi-bit messages match one another~~.

bit messages as correct only if the two multi-bit messages match one another.

The multi-bit message preferably comprises at least four data bits.

Ins. A4

Further advantages and individual features are presented in the following description of an embodiment, including the following diagrams:

FIG 1: a data transfer system,

FIG 2: a data transfer, and

FIG 3: a security unit.

Ins. A5

A

According to FIG 1, a data transmission system includes ~~comprises~~ a secure computer 1 and a number of input/output units 2 to 4. The secure computer 1 is designed in the present case as an error-protected stored-program control. A stored-program control of this type is manufactured and sold, e.g. by Siemens AG under the designation SIMATIC S5-95F.

The input/output units 2, 3 are conventional input/output units, by means of which up to four binary signals can be processed per unit. The input/output unit 4 on the other hand is a security unit. It can process precisely one data element. However, the security unit 4 could essentially process more data elements. It is crucial that it processes at least one data element less than the data bits transferred to it. This redundant data bit can then be used to check the data transfer system.

The input/output units 2 to 4 are connected to a serial bus system 5. Furthermore, a bus control unit 6, which

in turn is connected to the secure computer 1, is connected to the bus system 5. To transfer data between the secure computer 1 and the input/output units 2 to 4, the secure computer 1 activates the bus control unit 6. The latter successively activates the input/output units 2 to 4 and transfers a multi-bit message 8 including ~~comprising~~ at least four data bits to the relevant activated input/output unit 2 to 4.

The format of a data transfer is shown in FIG 2. According to FIG 2, the bus control unit 6, following a start bit 7′ and a checkbit 7″, first sends an address 7 via the bus system 5 in order to activate one of the input/output units 2 to 4. It then sends the multi-bit message 8, which includes ~~comprises~~ five data bits. The first data bit is a changeover bit, which is processed internally by the activated input/output unit 2 to 4. The second to fifth data bits are the actual data. The multi-bit message 8 is followed by a checkbit 8′ and an end bit 8″.

The activated input/output unit 2 to 4 sends a response 9, including ~~comprising~~ four data bits, following a start bit 7′. The response 9 is again followed by a checkbit 8′ and an end bit 8″.

The address 7 is incremented by the bus control unit 6 after each data transfer, until all input/output units 2 to 4 are activated. The input/output units 2 to 4 are then reactivated with the lowest address, and the cycle restarts.

According to FIG 3, the security unit 4 is designed in the present case as an output unit for activating an

output 10. Information indicating whether the output 10 should or should not be activated is therefore transferred by the bus control unit 6 to the security unit 4. The output 10 may be activated only if a

secure condition of a controlled system or a controlled machinery exists. The controlled system or the controlled machinery must not therefore pose any danger. Otherwise, the output 10 must be switched immediately to the non-activated condition.

To determine the control signal for the output 10, the security unit 4 first evaluates the second data bit of the transferred multi-bit message 8. The output 10 will be activated only if the data bit has the value one. Otherwise, the output 10 is switched to the secure, non-activated condition.

The third and fourth data bits are insignificant for the security unit 4 in the present case. However, further outputs could be activated with them if necessary.

The fifth data bit of the multi-bit message 8 is a checkbit. It is fed to a timer 13. The timer 13 is in each case reset when the checkbit fed to it alternates in relation to the checkbit previously fed to it. If, however, the checkbit retains its value, the timer 13 will expire at the end of a predefined monitoring period. In this case, the timer 13 transfers a zero signal to an AND circuit 12, so that the output 10 is also switched in this case to the non-activated condition. In this case also, an insecure condition of the controlled system or controlled machinery is therefore avoided. The monitoring period is defined in such a way that, on the one hand, in the case of correct (cyclical) bus traffic, the timer 13 is always reset in good time before it expires. ~~and,~~ Further on the other hand, in the case of incorrect bus traffic, the output 10 is switched to the non-activated condition at the

A

latest after a system-specific or machine-specific response time.

As is furthermore shown, the security unit 4 is designed in a redundant manner. It therefore has two bus modules 14, so that it can be activated under two different addresses. A separate multi-bit message 8 is, in each case, transferred to each of the bus modules 14 under its own address. Each of the bus modules 14 autonomously evaluates the multi-bit message 8 transferred to it and activates its AND circuit 12 accordingly.

The outputs 10 of the two bus modules 14 are connected in series. In the result, the transferred multi-bit messages 8 are therefore interpreted as correct only if they match one another. The security of the data transfer can be even further increased if the multi-bit messages 8 are transferred to the bus modules 14 inversely in relation to one another.

The bus modules 14 are reciprocally connected via switches 15. Each of the bus modules 14 therefore recognizes the switching condition of the respective other bus module 14. In their responses 9, the bus modules 14 can therefore feed not only their own switching condition, but also the switching condition of the respective other bus module 14, back to the secure computer 1. The security of the data transfer system is therefore even further increased.

A data transfer system with a single security unit 4, designed as an output unit for activating an output 10, has been described above. However, a plurality of security units can of course be connected to the bus system 5. The security units can also be designed as secure input units.